Zeitschrift: L'Enseignement Mathématique

Band: 45 (1999)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UNE MAJORATION DE LA LONGUEUR DES POLYNÔMES CYCLOTOMIQUES

Kapitel: 2. DÉMONSTRATION DU THÉORÈME 1

Autor: NICOLAS, Jean-Louis / TERJANIAN, Guy

DOI: https://doi.org/10.5169/seals-64451

Dans [5] (cf. aussi [3]), les polynômes

$$M_n(X) = (X+1)^n - X^n - 1 \tag{15}$$

sont appelés *polynômes de Cauchy-Mirimanoff*. Lorsque $n \geq 3$ est premier, on a $M_n(X) = -(X+1)P_n(-X)$. Cauchy a montré que

$$M_n(X) = X(X+1)^{a_n}(X^2+X+1)^{b_n}H_n(X) \tag{16}$$

avec $a_n = b_n = 0$ si n est pair, et, si n est impair, $a_n = 1$ et $b_n = 0, 2, 1$ suivant que $n \equiv 0, 1, 2 \bmod 3$. Il est conjecturé que $H_n(X)$ est irréductible pour tout $n \geq 2$. On sait que (cf. [5]), lorsque n est premier, $n \geq 9$, $H_n(X) = E_n(-X)$ est réductible modulo p pour tout p premier.

G. Terjanian conjecture que le polynôme E_m défini par (13) est irréductible sur les rationnels pour tout m. Cette conjecture a été vérifiée jusqu'à $m = 264$ (cf. [11], p. 93) et à l'aide du système de calcul formel *Maple*®, nous avons pu étendre les calculs jusqu'à $m = 1000$ par une méthode que nous expliquerons au paragraphe 3. En direction de cette conjecture, nous démontrerons comme conséquence du théorème 1

THÉORÈME 2. *Soit z une racine de l'unité telle que $P_m(z) = 0$, où le polynôme P_m est défini par (12) et $m \geq 2$. Alors, z est d'ordre 6, autrement dit, $z^2 - z + 1 = 0$.*

La démonstration du théorème 2 fera l'objet du paragraphe 3.

Une conjecture sans doute plus facile que celle de l'irréductibilité du polynôme E_m est la suivante : Est-ce-que toute racine multiple de P_m est une racine 6-ième de l'unité ? Nous avons vu que $\exp(-\frac{2i\pi}{3})$ est racine double de P_m pour une infinité de valeurs de m, par exemple les nombres premiers m qui vérifient $m \equiv 1 \bmod 6$.

2. DÉMONSTRATION DU THÉORÈME 1

LEMME 1. *Soit $\omega'(n)$ le nombre de facteurs premiers impairs distincts de n, et ε un nombre réel positif. On pose*

$$n_0 = n_0(\varepsilon) = \prod_{3 \leq p \leq \exp(1/\varepsilon)} p\,.$$

Alors, pour tout $n \geq 1$, on a

$$\omega'(n) \leq \varepsilon \log(n) + (\omega'(n_0) - \varepsilon \log(n_0))\,.$$

Cas particulier: $\varepsilon = 0,32/\log 2$. *On a pour tout* $n \geq 1$

$$\omega'(n) \leq \frac{0,32}{\log 2} \log n + 0,852\,.$$

ou encore

$$2^{\omega'(n)} \leq 1,81 n^{0,32}\,.$$

Démonstration. Nous utiliserons implicitement la méthode des “nombres hautement composés supérieurs” introduite par Ramanujan (cf. [9], paragraphe 32).

Pour $\alpha \in \mathbf{N}$, on définit $f(\alpha) = 1$ si $\alpha \geq 1$ et $f(\alpha) = 0$ si $\alpha = 0$. La fonction ω' est additive; on a $\omega'(2^\alpha) = 0$ et $\omega'(p^\alpha) = f(\alpha) \leq \alpha$ pour tout $\alpha \in \mathbf{N}$, et p premier impair. Soit $\mathcal{P}$ l'ensemble des nombres premiers. On écrit

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}\,, \qquad \alpha_p \geq 0$$

et il s'ensuit que

$$\begin{aligned}
&\omega'(n) - \varepsilon \log(n) - (\omega'(n_0) - \varepsilon \log(n_0)) \\
&\quad = -\varepsilon \alpha_2 \log 2 + \sum_{3 \leq p \leq \exp(1/\varepsilon)} \big(f(\alpha_p) - \varepsilon \alpha_p \log p - (1 - \varepsilon \log p)\big) \\
&\qquad + \sum_{p > \exp(1/\varepsilon)} \big(f(\alpha_p) - \varepsilon \alpha_p \log p\big) \\
&\quad \leq \sum_{3 \leq p \leq \exp(1/\varepsilon)} (f(\alpha_p) - 1)(1 - \varepsilon \log p) + \sum_{p > \exp(1/\varepsilon)} f(\alpha_p)(1 - \varepsilon \log p) \leq 0\,.
\end{aligned}$$

Pour $\varepsilon = 0,32/\log 2$, on a $\exp(1/\varepsilon) = 8,724\ldots$, $n_0 = 3 \cdot 5 \cdot 7 = 105$ et $\omega'(n_0) - \varepsilon \log(n_0) \leq 0,852$.

Rappelons d'abord les formules de calcul de Φ_m (cf. [6], 4.6.2, exercice 32):

(17) pour p premier, $\qquad \Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$

(18) si p premier divise n, $\qquad \Phi_{pn}(X) = \Phi_n(X^p)$

(19) si p premier ne divise pas n, $\qquad \Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$

(20) si n est impair, $\qquad \Phi_{2n}(X) = \dfrac{\Phi_n(X^2)}{\Phi_n(X)} = \Phi_n(-X)\,.$

Soit $n = \ker m$ le noyau impair de m : si $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $3 \le p_1 < p_2 < \dots < p_k$, on a $n = p_1 p_2 \dots p_k$. Les formules (18) et (20) montrent que

$$\beta(m) = \beta(n). \tag{21}$$

Démontrons d'abord que le théorème 1 est vrai lorsque $k = \omega'(m) \le 2$.

- Si $k = 0$, $m = 2^{\alpha}$ et par (21), $\beta(m) = \beta(1) = 2$, tandis que $\varphi(m) = 2^{\alpha-1}$ et (4) est vérifié pour $\alpha \ge 3$. Les exceptions sont donc $m = 1, 2, 4$.
- Si $k = 1$, on a $m = 2^{\alpha} p_1^{\alpha_1}$, et par (21), et (17), $\beta(m) = \beta(n) = \beta(p_1) = p_1$ et $\varphi(m) \ge (p_1 - 1)$. L'inégalité

$$p_1 < (\sqrt{2})^{p_1 - 1}$$

est vérifiée pour $p_1 \ge 7$. Pour $p_1 = 3$ ou 5, on a

$$p_1 < (\sqrt{2})^{2(p_1 - 1)}$$

et cela démontre (4) pour $m = 2^{\alpha} p_1$, avec $\alpha \ge 2$ ou pour $m = 2^{\alpha} p_1^{\alpha_1}$, avec $p_1 = 3$ ou 5, $\alpha = 0$ ou 1, et $\alpha_1 \ge 2$. Les exceptions sont donc $m = 3, 5, 6, 10$.
- Si $k = 2$, on sait depuis Migotti (cf. [7]) que dans (2) les coefficients $a_{m,i}$ valent -1, 0 ou 1 et cela entraîne

$$\beta(m) \le 1 + \varphi(m). \tag{22}$$

Pour $t \ge 6$, on a $1 + t \le (\sqrt{2})^t$, et donc (22) implique (4) dès que $\varphi(m) \ge 6$. Or, lorsque $k = 2$, on a $\varphi(m) \ge (p_1 - 1)(p_2 - 1) \ge 2 \cdot 4 = 8$.

On peut maintenant supposer $k \ge 3$. Par (10), on a

$$\log \beta(m) \le \frac{2^{k-1}}{k} \log m$$

et par (11), on a

$$\varphi(m) \log(\sqrt{2}) \ge \frac{1}{2} \frac{m}{k+2} \log 2.$$

Pour prouver (4), il suffit donc d'assurer

$$\frac{2^{k-1}}{k} \log m < \frac{1}{2} \frac{m}{k+2} \log 2$$

ou encore

$$2^k \left(1 + \frac{2}{k}\right) < \log 2 \frac{m}{\log m}$$

et comme $k \geq 3$, et en appliquant le lemme 1,

$$1,81 m^{0,32} < \frac{3 \log 2}{5} \frac{m}{\log m} .$$

Finalement, comme $\frac{5 \times 1,81}{3 \log 2} < 4,36$, il suffit de montrer

$$m^{0,68} - 4,36 \log m > 0 .$$

L'inégalité ci-dessus est vérifiée pour tout $m \geq 75$ et comme le plus petit nombre m avec $k = \omega'(m) \geq 3$ est $105 = 3 \cdot 5 \cdot 7$, (4) est démontrée pour tous les m avec $k = \omega'(m) \geq 3$, et cela termine la preuve du théorème 1.

3. Démonstration du théorème 2

D'abord, on a $P_m(1) = \Phi_m(1)$ et par (14), 1 n'est pas racine de P_m pour $m \geq 2$. De même, -1 n'est pas racine de P_m : lorsque m est impair, (1) donne

$$\Phi_m(-1) = \prod_{d|m} 2^{\mu(d)} = 2^{\sum_{d|m} \mu(d)} = 1$$

dès que $m \geq 3$. Les formules (18), (20) et (14) montrent que pour $m \geq 3$, $\Phi_m(-1)$ est impair, sauf pour $m = 2^n$ où l'on a $\Phi_m(-1) = 2$. On ne peut donc avoir $P_m(-1) = 0$.

Soit maintenant z une racine de l'unité différente de 1 et -1 et d'ordre $r \neq 6$ telle que $P_m(z) = 0$. Par conjugaison, les autres racines d'ordre r sont aussi racines de P_m. Soit k l'ordre de $-z$. (Si $r \equiv 0 \bmod 4$, on a $k = r$; si $r \equiv 2 \bmod 4$, on a $k = r/2$; si r est impair, on a $k = 2r$.) On a $P_m(-\exp(\frac{2i\pi}{k})) = 0$, et comme $\varphi(m)$ est pair, il vient

$$\Phi_m\Big(-\exp\Big(\frac{2i\pi}{k}\Big)\Big) = \Big(\exp\Big(\frac{2i\pi}{k}\Big) + 1\Big)^{\varphi(m)} .$$

D'où en prenant les modules,

$$\beta(m) \geq \Big|\Phi_m\Big(-\exp\Big(\frac{2i\pi}{k}\Big)\Big)\Big| \geq \Big(2 \cos \frac{\pi}{k}\Big)^{\varphi(m)} .$$

Comme $z^2 \neq 1$, on a $k \neq 1, 2$. On a $k \neq 3$, sinon, z serait d'ordre $r = 6$. Donc $k \geq 4$ et

$$\beta(m) \geq (\sqrt{2})^{\varphi(m)} .$$

Par le théorème 1, m doit être égal à $2, 3, 4, 5, 6$ ou 10. Le calcul direct des polynômes P_m pour ces valeurs montre qu'ils vérifient aussi le théorème et cela achève la démonstration du théorème 2.